Wherefore, what is claimed is:

1. A computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of:

generating a request for services of a service provider at a user's computing device;

generating a challenge at a user's computing device;

the user answering the challenge;

said user's computing device evaluating said user's answer to the challenge and attaching a digital signature thereto if said user's answer is correct;

sending said request for services including said digital signature from the user to a service provider;

said service provider evaluating said user's request for services and digital signature; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digital signature.

2. The computer-implemented process of Claim 1 wherein the user's computing device comprises a trusted computing environment comprising a challenge generator and a secret key.

3. The computer-implemented process of Claim 2 wherein the secret key is used to generate the digital signature.

4. The computer-implemented process of Claim 1 wherein symmetric encryption techniques are used to encrypt at least one of said request for services and digital signature.

5. The computer-implemented process of Claim 1 wherein asymmetric encryption techniques are used to encrypt at least one of said request for services and digital signature.

6. The computer-implemented process of Claim 3 wherein said digital signature identifies and authenticates the user's trusted device and message data.

7. The computer-implemented process of Claim 3 wherein the message data includes the user's answer to the challenge.

8. The computer-implemented process of Claim 1 wherein the process action of generating a challenge at a user's computing device comprises the actions of:

the user generating a preliminary request for services message to said service provider;

generating a cryptographic hash using data from said preliminary request for services message; and

using said cryptographic hash to generate said challenge.

9. The computer-implemented process of Claim 8 wherein the cryptographic hash is used to generate a short sequence of alphanumeric characters which is rendered into a visual image that the user is to identify.

10. The computer-implemented process of Claim 1 wherein said service provider's determination of whether to allow said user access to said service provider's services is used for one of:

assigning an email account;

validating an input in a poll;

using a search engine;

using a chat room; and

accessing data on a website.

11. A system for creating a non-interactive human proof, the system comprising:

a general purpose computing device; and

a computer program comprising program modules executable by the computing device, wherein the computing device is directed by the program modules of the computer program to,

generate a challenge for a computer user using said user's computing device that includes a trusted computing device;

require a computer user to answer the challenge;

send the computer user's answer to the challenge to a service provider with a request to access the computer user's services.

12. The system of Claim 11 further comprising modules of a computer program to:

verify the user's answer to the challenge; and

if the user's answer is correct, allow the user access to services provided by the service provider.

13. The system of Claim 11 wherein said trusted computing device comprises a challenge generator and a secret key.

14. The system of Claim 13 wherein the challenge is generated by

the user generating a preliminary request for services message to said service provider;

generating a cryptographic hash using data from said preliminary request for services message; and

using said cryptographic hash to generate said challenge.

15. The system of Claim 14 wherein the cryptographic hash is used to generate a sequence of alphanumeric characters which is rendered into a visual image for the user to identify.

16. A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:

generating a challenge at a user's computing device for the user using the a trusted computing device resident on the user's computing device;

the user answering the challenge;

sending a request for services including a digitally signed assertion that the challenge has been successfully answered;

said service provider evaluating said user's request for services and digitally signed assertion; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digitally signed assertion.

17. The computer-implemented process of Claim 16 wherein the process action of generating a challenge comprises generating a challenge that requires that significant resources be expended to answer the challenge.

18. The computer-implemented process of Claim 17 wherein the trusted computing device reports back to the user a partial digital signature, and wherein the remainder of the digital signature is rendered as a challenge.

19. The computer-implemented process of Claim 17 wherein the user computes the remainder of the partial signature.

20. The computer-implemented process of Claim 19 wherein the user's answer to the challenge when combined with the given portion of the digital signature forms the digitally signed assertion.

21. The computer-implemented process of Claim 16 wherein said challenge is generated using information extracted from said user's request for services.

22. The computer-implemented process of Claim 21 wherein the information extracted from said user's request for services includes one of: message content; date; time; a sender's name; the sender's address; the recipient's name; the recipient's address; and an answer to a challenge generated by the challenge generator.

23. A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:

generating a challenge for a user at the user's computing device using a trusted computing device resident on the user's computing device by generating a cryptographic hash of information that is extracted from a message the user generates requesting services from a service provider;

the user answering the challenge;

the user receiving a digitally signed assertion;

the user sending a request for services including a digitally signed assertion that the challenge has been successfully answered;

said service provider evaluating said user's request for services and digitally signed assertion; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digitally signed assertion.

24. The computer-implemented process of Claim 23 wherein the cryptographic hash is rendered into a string of alphanumeric characters that are presented as a visual image as said challenge to the user.

25. The computer-implemented process of Claim 24 wherein said alphanumeric characters that are presented as a visual image are not recognizable by an optical character recognition program.

26. A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:

generating a challenge for a user that comprises a partial digital signature using a trusted computing device resident at a trusted third party;

the user answering the challenge to complete the digital signature;

the user sending a request for services including the complete digital signature;

said service provider evaluating said user's request for services and digital signature; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digital signature.

27. The computer-implemented process of Claim 26 wherein the user's computing device computes the portion of the digital signature necessary to complete the partial digital signature.

28. A computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of:

generating a request for services of a service provider at a user;

generating a challenge at a trusted third party and providing it to said user;

the user answering the challenge;

said trusted third party evaluating said user's answer to the challenge and attaching a digital signature thereto if said user's answer is correct;

sending said request for services including said digital signature from the trusted third party to a service provider;

said service provider evaluating said user's request for services and digital signature; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digital signature.

29. A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:

a user generating a request for services of a service provider and sending said request to a third party;

said third party generating a challenge for the user;

the user answering the challenge and sending said answer to said third party;

sending the user's request for services including a digital signature identifying the third party and the user's answer to the service provider;

said service provider evaluating said user's answer and digital signature; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's answer and digital signature.

30. A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:

a user generating a request for services of a service provider and sending said request to a trusted third party;

said third party generating a challenge that requires said user to expend significant resources to answer the challenge and providing the challenge to the user;

the user answering the challenge and providing the answer to said trusted third party;

sending the request for services including a digitally signed assertion that the challenge has been successfully answered to a service provider;

evaluating said request for services and digitally signed assertion; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digitally signed assertion.

31. The computer-implemented process of Claim 30 wherein the trusted third party reports back to the user a partial digital signature, and wherein the remainder of the digital signature is rendered as a challenge.

32. The computer-implemented process of Claim 31 wherein the user computes the remainder of the partial signature as the answer to the challenge.

33. The computer-implemented process of Claim 31 wherein the user's answer to the challenge when combined with the given portion of the digital signature forms the digitally signed assertion.

33. The computer-implemented process of Claim 30 wherein said challenge is generated using information extracted from said user's request for services.

34. The computer-implemented process of Claim 30 wherein the trusted third party reports back to the user a corrupted digital signature whose correction is rendered as a challenge.

35. A computer-readable medium having computer-executable instructions for determining whether a computer user is human or a computer program, comprising program modules for:

generating a request for services of a service provider at a user's computing device;

generating a challenge at a user's computing device ;

the user answering the challenge;

said user's computing device evaluating said user's answer to the challenge and attaching a keyed hash thereto if said user's answer is correct;

sending said request for services including said keyed hash from the user to a service provider;

said service provider evaluating said user's request for services and keyed hash; and

said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said keyed hash.

36. The computer-readable medium of Claim 35 wherein the user's computing device comprises a trusted computing environment comprising a challenge generator and a secret key.

37. The computer-readable medium of Claim 35 wherein said keyed hash identifies and authenticates the user's trusted device and message data.

38. The computer-readable medium of Claim 35 wherein the message data includes the user's answer to the challenge.

39. The computer-readable medium of Claim 35 wherein the process action of generating a challenge at a user's computing device comprises the actions of:

the user generating a preliminary request for services message to said service provider;

generating a cryptographic hash using data from said preliminary request for services message; and

using said cryptographic hash to generate said challenge.

40. The computer-readable medium of Claim 39 wherein the cryptographic hash is used to generate a short sequence of alphanumeric characters which is rendered into a visual image that the user is to identify.

41. The computer-readable medium of Claim 35 wherein said service provider's determination of whether to allow said user access to said service provider's services is used for one of:

assigning an email account;

validating an input in a poll;

using a search engine;

using a chat room; and

accessing data on a website.